Authentication and Authorization of Users and Services in Federated SOA Environments – Challenges and Opportunities

Bartosz Jasiul, Joanna Sliwa, Rafał Piotrowski, Robert Goniacz, Marek Amanowicz
Military Communication Institute
ul. Warszawska 22A, 05-130 Zegrze
POLAND
Tel.: +48 22 688 55 92, Fax.: +48 22 688 55 89

E-mail: { b.jasiul; j.sliwa; r.piotrowski; r.goniacz; m.amanowicz }@wil.waw.pl

ABSTRACT

Problem of user authentication and authorization is usually being solved in a single system. Federated environment assumes heterogeneity of systems, which brings the problem of mutual users and services authentication and authorization. In this article the authors presented security requirements for cross domain information exchange in federated environments. Special attention was paid to authentication and authorization of users and services. As opportunities there were presented solutions verified at multinational experimentations and exercises.

1.0 INTRODUCTION

The main tenet of net-centricity is to achieve information superiority by sharing reliable information collected from various sources, creating situational awareness and distributing it among mission participants, across domains, context and organizational boundaries. However improvement of collaboration and information sharing in highly dynamic, unpredictable NEC (Network Enabled Capability) environment is a great challenge. It assumes transfer of information between users of so called Federation of Systems with required quality of service and security independently of the underlying infrastructure as well as common access to relevant information by the authorized users.

Federation-of-Systems (FoS) capability derives from the strategy for developing the networking and information sharing aspects of NATO NEC (NNEC) and focuses on joining together networking systems and core information systems from NATO and NATO nations. The FoS concept refers to a set of different systems, which are not centrally managed, but are so connected or related so as to produce results beyond those achievable by the individual systems alone [4]. This implies that NII consists of national Networking and Information Infrastructures (NIIs) segments and a NATO Networking and Information Infrastructure (NNII), which together will provide capabilities that no one system can provide by itself. This concept is similar to the one known from Internet, where there is no central control, and synergy for the federation is achieved through collaboration and cooperation.

Operational capabilities needed to conduct modern military operation from the technical point of view impose the use of flexible, adaptable architecture enabling seamless information exchange in dynamically changing, unpredictable Federation of Systems. In order for these requirements to be satisfied NATO recommends the use of Service Oriented Architectures (SOAs), that succeeded in commercial world lately and are seen as crucial NEC enabler [1][2][3][4].

Service orientation is a conceptual architecture which asymmetrically provides services to arbitrary service consumers facilitating information sharing in heterogeneous environment, and thus supports to some degree aspects of net-centricity. SOA can make military information resources available in the form of services that can be discovered and used by all mission participants that do not need to be aware of

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Authentication and Authorization of Users and Services in Federated SOA Environments Challenges and Opportunities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Military Communication Institute ul. Warszawska 22A, 05-130 Zegrze POLAND**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
Problem of user authentication and authorization is usually being solved in a single system. Federated environment assumes heterogeneity of systems, which brings the problem of mutual users and services authentication and authorization. In this article the authors presented security requirements for cross domain information exchange in federated environments. Special attention was paid to authentication and authorization of users and services. As opportunities there were presented solutions verified at multinational experimentations and exercises.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**12**	

these services in advance. That is why the NII strategy assumes that the system infrastructure will be implemented as a Federation of Systems, involving the use of SOA to expose software functions as consumable services that can be discovered and invoked across the network.

SOA's greatest advantage is the ability of seamless information exchange based on different policies and loose coupling of its components. This can be realized however by the widespread use of open standards. One of the most mature realizations of SOA assumes application of Web Services (WS) – the most successful implementation of this paradigm.

WSs, based on eXtensible Markup Language (XML), SOAP, Web Services Description Language (WSDL) and related open standards, implemented in national systems, allow data and applications to interact without human intervention through dynamic, ad-hoc coalition connections. WSs are in fact described by a wide range of standards that deal with different aspects of WS realization, transport, orchestration, semantics etc. They provide means to build very flexible environment that is able to dynamically link different system components to each other. The most important and obvious advantage of this solution is its natural applicability to FoS, where it can be implemented in a wide variety of communications systems, can co-exist with other technologies and software design approaches [5], and be adopted in evolutionary way without the need to modify legacy systems.

2.0 SECURITY CHALLENGES

Sharing information among mission participants in FoS imposes many technological interoperability on data, application and communications levels. What is more, unpredictability of this environment, mobility and dynamic nature of NEC operations impose several threats that do not occur in a system managed by single administration.

The security challenges inherent to the Web services approach are alarming and unavoidable [1]. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are being seen by the Security Officers as threatening or even forbidden with traditional security models and controls. Even the idea of ubiquitous information sharing with different security classification between domains building FoS is currently seen as risky.

Security objectives [7] for federated SOA-based systems are the same as for all IT communication means and covers confidentiality, integrity, access control, non-repudiation, accountability and availability. Such attitude guarantees controlled access to network elements, services and applications for identified users.

Both, identification of users and services across domains and providing appropriate information for making authorization decision rise interoperability problems. It is even more visible in SOA- based systems where services can be invoked by users not known in design time, so that SOA-based systems must face up additional requirements[6]:

- balancing information sharing with security,
- trust propagation between federated systems
- minimizing vulnerabilities (e.g. in terms of software development)
- providing access to system resources for unanticipated users.

First of all, in order for the users to share information and use these received, they must be sure that the source and sink are reliable. Information can be though shared only among users/devices that have been identified and are approved for this kind of data. Only cross-domain authentication and authorization, based on trust relation between security providers and appropriate identity management are able to fulfil initial security requirements for FoS (see Fig.1).

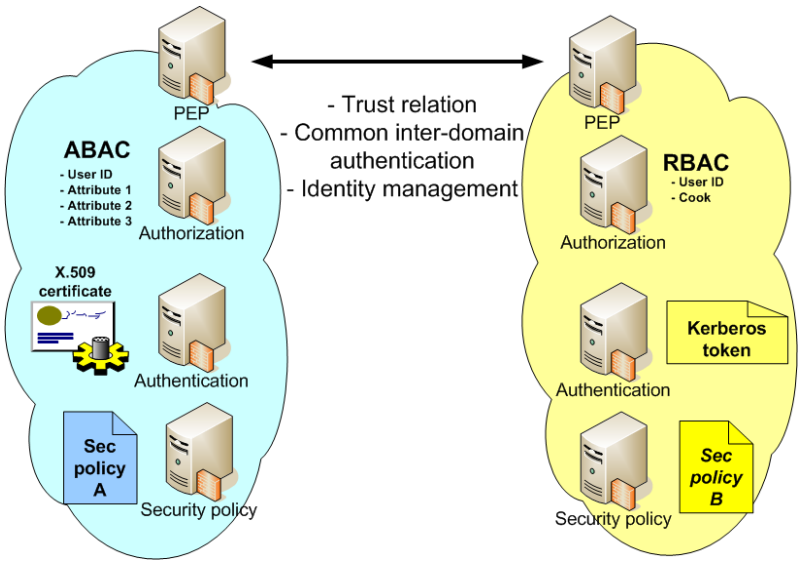

Fig. 1 Cross-domain authentication and authorization of users and services. Intradomain and interdomain security mechanisms.

As shown in Fig.1, in national C4I system access to information is controlled and granted only for authenticated and entitled users from this domain. Access control is an internal issue of the system and can be realized in different ways. Authorization decision is made locally and usually bases not only on user rights, attributes but also invoked web service attributes and valid security policy. The set of user attributes required for making decision may differ depending on the system implementation. The mechanism usually secures all information flows inside the system.

Authentication mechanism is to confirm identity of a user or service (see Fig.3). To perform access control, Web services need to identify and authenticate requesters. In FoS it can be performed by different means. Each domain can have their own authentication services that base on login/password, X.509 certificates, biometric data, etc. Authentication services in different domains must interoperate with each other and accept identity confirmation issued in the other domain (some kind of a token). It must be emphasised that the user must be appropriately identified across domain boundaries.

Access to services can be granted or denied based on the authorization service decision which can use different access control (AC) models (e.g Role Based - RBAC, Attribute Based - ABAC, Policy Based - PBAC, Risk Adaptive - RAAC). In real life scenarios domains can use different combinations of the above, applying rules that are defined for this particular system. These rules can be generally called *Policy of information sharing*, which do not imply that this is PBAC.

In disrupted networks where connections are not stable, to achieve reliability of the system distributed Policy repository implementation is recommended. This solution allows all Policy Decision Points (PDPs) present in the system to perform authorization decision invoking local copy of the Policy. It should be noted that policy rules may change dynamically during the system and mission lifetime (e.g. domains or users may become untrusted). Rules may change as a result of administrator activities as well as actual risk assessment. These changes must be immediately distributed to all Policy repositories employed in the system. Effective policy database replication mechanism is essential to enable all PDPs realize access control decisions according to current and valid rules.

Some users may frequently request particular set of services provided by own or federated domains. Getting authorization each time user queries any resource may overload the security services and can make the process of retrieving results more cumbersome. Thus important issue is provision of a

mechanism allowing users to authenticate with one system to a single point (the user's identity provider) and, on the basis of that authentication statement (usually being some kind of a token), use other services and applications within SOA. This mechanism is called single sign-on (SSO) (see Fig.2). SSO allows users to have more flexible access to system resources which can limit the time needed to get necessary data and number of authentication requests.

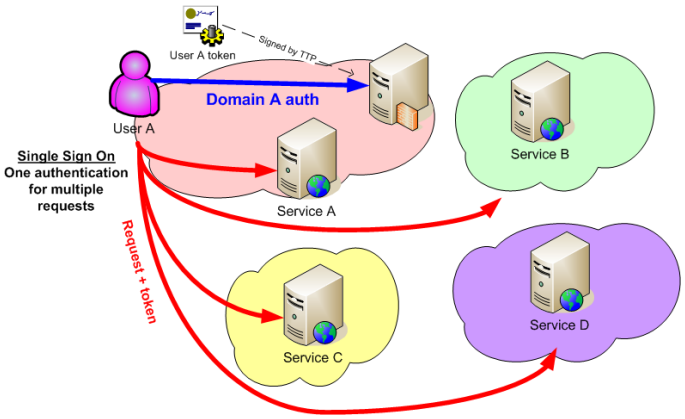

Fig. 2 Single sign on in FoS

As it was already stated, one of the core requirements for sharing information on FoS is trust relation among cooperating nations. All entities involved in a transaction or process must trust one another. A level of trust must be in place for the parties to be willing to co-operate in common operations and to exchange sensitive information in a timely manner. The willingness to share and accept information depends heavily on trusting the receiver and the provider of information.

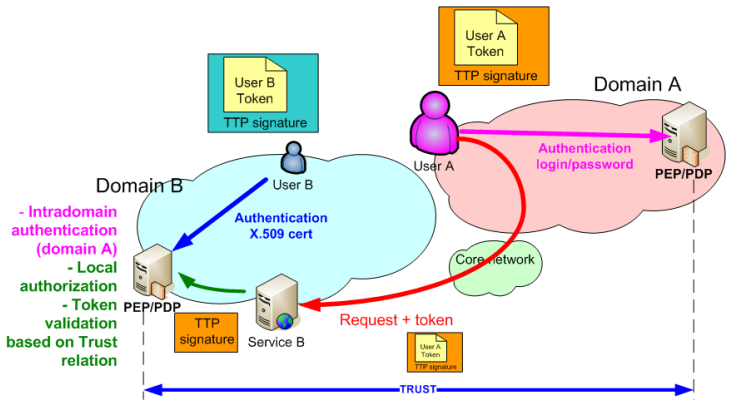

Fig. 3 Authentication, authorization and trust relation in cross-domain information sharing

There are several trust relationship models that can be used in WS security. The most useful is federation of trust, which bases on federated identity management. A federated trust model allows users and web services from various domains to interact with some level of security. It is based on both the brokered and bilateral trust models. Particular domains use so called Trusted Third Party (TTP) that is to certify that service or requester can be trusted within the domain. Each domain has its own TTP and TTPs of these domains have mutual relationships. Establishing trust is very important during client-provider transactions as well as in service-to-service interactions.

Provision of security in terms of authentication and authorization in federated environment goes beyond the challenges presented above. Cross-domain solutions that provide identification of users, are able to

present and then analyse their credentials for the purpose of authorization usually base on assertions or tokens that prove local authentication and enable granting access to the resource. The problem gets more complicated when we imagine service composition (the chain of services) when one application requests data from another one. In this case the entity that initiated the process should be granted the access to particular resources. The problem can be solved by identity delegation, that assumes passing identity of requesting user through the service chain, however its technical realisation can be cumbersome in the range of one system, not mentioning federated environment.

3.0 OPPORTUNITIES

In order to show opportunities of authentication and authorization in federated environment we present results of experiments that were carried out during preparation for multinational experimentation MNE 6 and demonstrated on Combined Warrior Interoperability Demonstration (CWID) in 2009. The solution covers the basic requirements for authentication and authorization of users and services and was used to share data between maritime systems supporting creating multinational interagency situational awareness on the sea. This section describes the cross-domain authentication and authorization solution that was implemented in two different domains independently, given existing local interdomain security mechanisms.

3.1 Description of the Trial

Authentication and authorization mechanisms in presented system are developed in Service Oriented Architecture as a set of loosely coupled security Web services. To ensure trust relation between heterogeneous domains forming federation of systems there was assumed mutual acknowledgement of Public Key Infrastructures (PKIs) approved in each domain.

When the user wants to get access to a resource located outside his domain, he needs to be authenticated in his own domain. In order to prove his authentication in the other domain he gets security assertion (some kind of a passport) consisting of user identity, public key and attributes. Local authentication can be made with different security mechanisms, e.g. id and password, Kerberos ticket, X.509 certificate. This solution guarantees independence of policy rules in each autonomous system. However assertion must be understandable to the cooperating system. The trust to the users is internal case of the system and may depend on authentication method, because there is a huge difference of efficiency between X.509 and e.g. id and password mechanism.

In presented solution X.509 certificates [9] were implemented for intradomain user authentication. Certificates based on open industry standards are supported on many platforms. Additionally X.509 certificates can be used to provide confidentiality and data origin authentication at the message and transport layer. Identity of particular participant in a message exchange is unique and can be confirmed by verification of signature made using X.509 certificates.

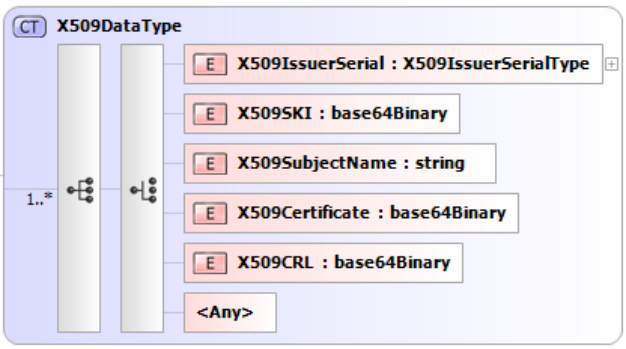

Fig. 4 X.509 Certificate schema

For cross-domain authentication Security Assertion Markup Language (SAML) [8] tokens were chosen. They carry X.509 credentials and additional values e.g. signatures and user attributes. SAML is an XML-based standard introduced by Security Services Technical Committee of the OASIS for exchanging authentication and authorization data between security domains. In presented model SAML assertions are transferred from identity provider (that can be e.g. Secure Token Service) to service provider. It must be noted that signatures included in SAML tokens guarantee message integrity and non-repudiation (signatures unable to fake identity of user and his attributes).

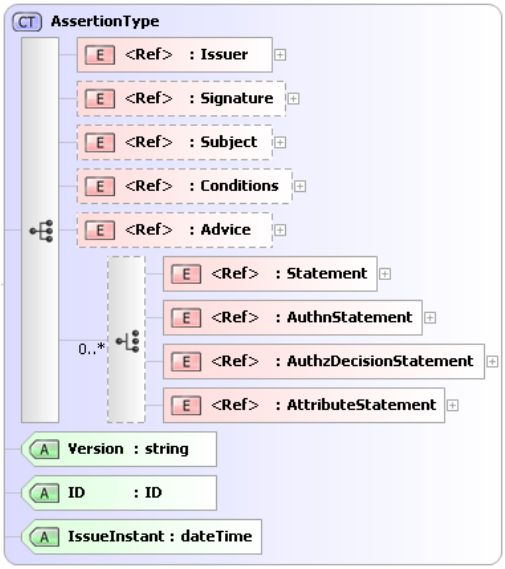

Fig. 5 SAML Assertion schema (green tags are for obligatory elements, red ones – for optional)

The advantage of utilizing SAML is its flexibility and adaptability to carrying variety of properties which can be used for securing communication. In fact only a few elements are mandatory in SAML assertion and the rest is optional. Assertion contains statements that the service provider uses to make access control decisions.

SAML provides three statements (see Fig. 5.):

- authentication – asserts to the service provider that the principal (e.g. STS, PEP) authenticated the requester at a particular time using a given method of authentication (e.g. user/password, biometric data, X,509 certificates, Kerberos, etc),

- attribute – provides attributed of requester that could be used to make access control decision,
- authorization decision statements – provides permissions for particular actions.

SAML assertion is composed of obligatory and optional elements. This allowed us to incorporate information about local authentication of the user based on X509 certificates and send user attributes for the purpose of authorization.

SAML assertion used for the trial consisted of the following elements:

- Issuer – the unique identifier of the requesting service provider / the unique identifier of STS, PEP;
- Subject – SOAP message source unique identifier (requester or a service provider);
  - Both issuer and subject data are extracted from X.509 certificates and consist of common name, organization unit, organization, country (CN, OU, O, C).
- Signature – a value obtained from signing the whole request / response message; it provides message integrity and guarantees non-repudiation;
- Conditions – validity period; it consists of values: NotBefore and NotOnOrAfter;
- Authentication statement – a method used to authentication of the user;
- Attribute statement - attributes of the user used for authorization e.g. military rank, function in organization, secrecy permissions.

3.2 Implementation of the Solution

Each request to a service must be augmented with appropriate SAML assertion with a token proving user authentication and its credentials necessary for local authorization. Such an assertion the user usually gets from so called Security Token Service, that is able to verify its identity (based on the local authentication mechanisms) and prepare appropriate SAML assertion, understandable to the requested site. Appropriately prepared SOAP message is sent to the service.

For the purpose of the trial a set of security services was implemented (see Fig.6). They are to provide cross-domain authorization and authentication based on trust relation. Policy Enforcement Point is treated as main SAML assertion processing module (engine). It analyses part of the SOAP message header i.e. SAML assertion and delegates tasks to particular auxiliary security modules: CertVerify Service, AuthorizationWS Service and KeyNegotiate Service. Together with PEP they create Core security services system.

PEP and auxiliary modules are implemented as Web services communicating with each other with SOAP messages. As mentioned before, PEP, with auxiliary services, is responsible for validating SAML assertions. It:

- validates X.509 certificate and digital signature of SOAP message embedded in assertion,
- extracts and validates user authorization attributes, and
- obtains symmetric crypto key from KeyNegotiation Service.

The certificate included in the SOAP message belongs to the requester and it is validated against public key of its authority which was bilaterally exchanged at the memorandum of co-operation (at the level of establishing trust). User attributes are credentials describing user place in the organization hierarchy. Depending on the level of trust between domains this credentials may be used to take appropriate authorization decision.

Key Negotiation Service is to exchange seeds that allows to calculate symmetric crypto key. It could be derived from shared secret values or from asymmetric computations. This crypto key is used to encrypt communication between the user and requested service, what fulfils confidentiality requirements.

If all of these processing stages return valid and correct values, PEP module, in turn, allows Web Service to proceed further proprietary operations. The only stated requirement from the service provider is to call PEP operations before processing any proper Web Service task, just after receiving SOAP message request. Implementation was based on open source Web Services frameworks and APIs e.g. JAX-WS Java API for Web Services, Bouncy Castle Java Cryptography API and EJBCA - Open Source PKI library.

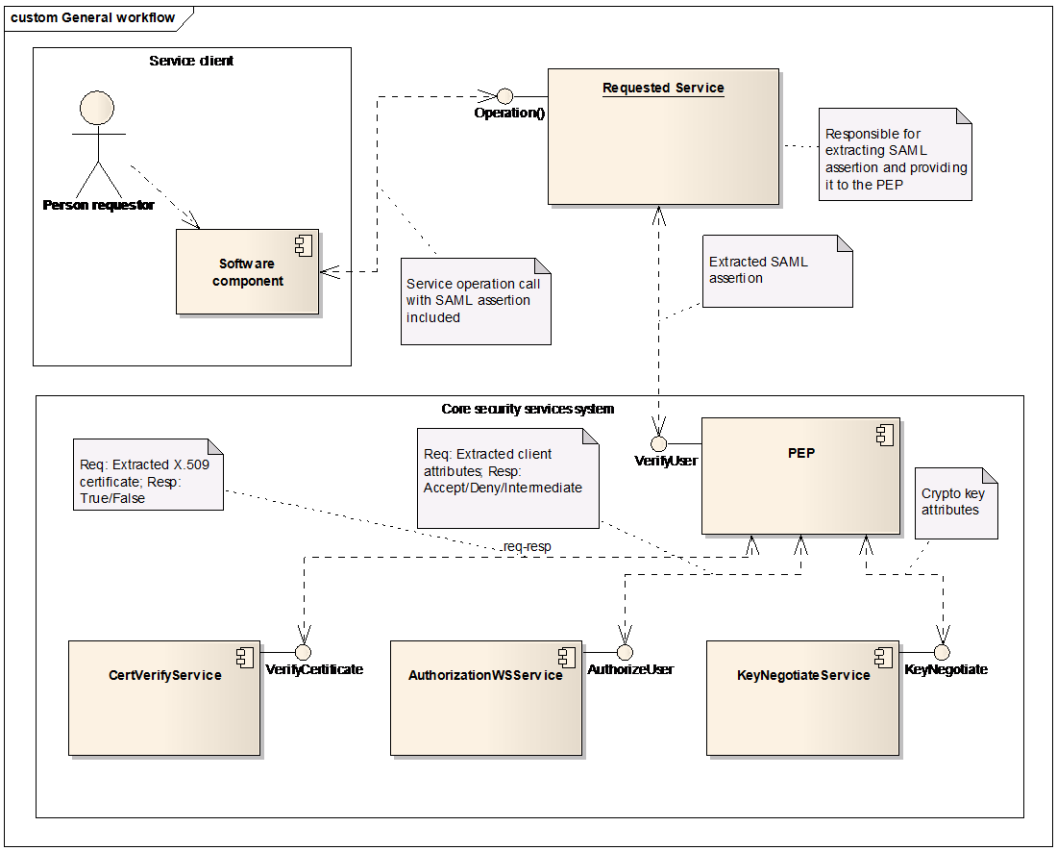

Fig. 6 Core security services system workflow diagram

Reverse processing workflow takes place while sending each of the SOAP response messages, e.g. to authenticate the service to the requester. After the client has had access granted requested service communicates with PEP in order to have its response message appropriately prepared. Just before sending Web Service response PEP is involved in preparation of the SAML assertion. It:

- gains user attributes and crypto key,
- prepare whole SOAP message including SOAP header.

This is implemented by using output handler (JAX-WS handler), which delegates the workflow to PEP. General logical workflow of processing request and response SOAP messages is presented in Fig.7.

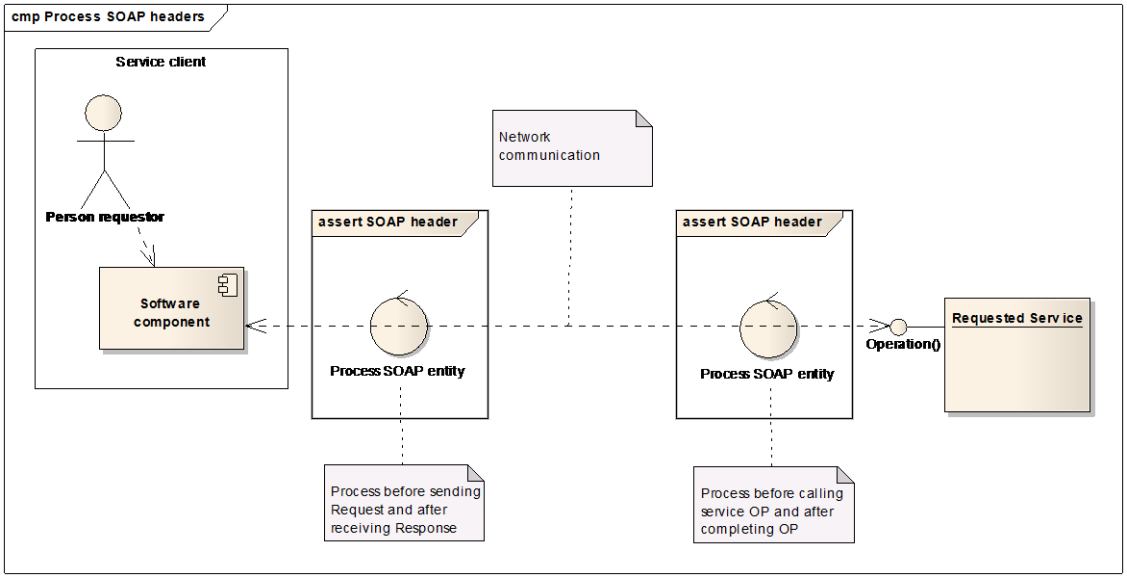

Fig. 7 Workflow of processing SOAP request and response messages

3.3 Verification of the Solution

General overview of tests carried out during workshops and CWID 2009 exercises is depicted in Figure 8. Tests and implementations were prepared and developed by Polish and Swedish teams engaged in realization of objective 4.2 titled Multinational Interagency Situational Awareness – Extended Maritime (MISA-EM), which is a part of sixth edition of MultiNational Experimentations (MNE-6).

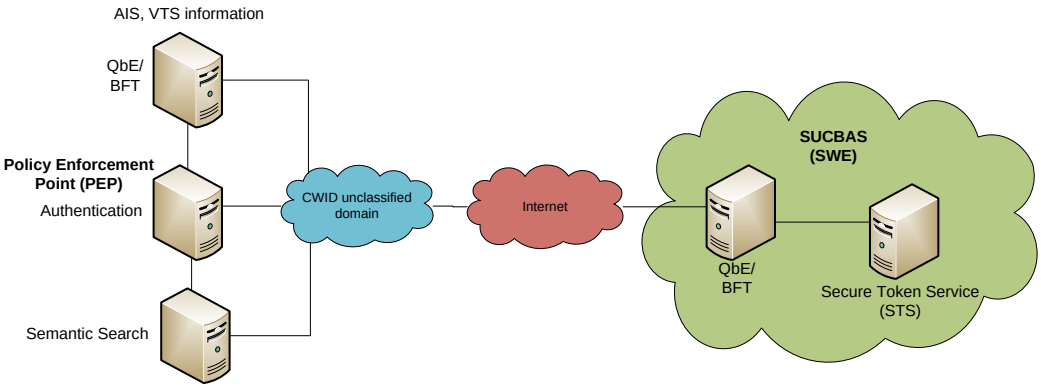

Fig. 8 CWID test infrastructure

It must be emphasized that Swedish and Polish implementation were prepared separately, without exchanging any line of code. General concept of cross-domain security solution for both realizations based on the same assumptions and was agreed before experiments. However software products and solutions of security Web Services are different. Swedish implementation does not include PEP, however its functionalities were adopted to security proxy service adding/removing security assertions and Secure Token Service (STS).

Tests covered a few scenarios. In the first scenario (see Figure 9.) Swedish side invokes Polish Blue Force Tracking (BFT) service. At the client side STS, provided exclusively by the Swedish side, was responsible for preparing appropriate SAML assertions embedded in the SOAP messages. After receiving by BFT

service provider, SAML assertion was analyzed by PEP, provided exclusively by the Polish side. In case of any errors (i.e. wrong or not valid X.509 certificates, not appropriate private keys, modifications injected into SOAP messages) PEP informs BFT provider about such a situation and processing chain can be stopped (access denied). In case of successful SAML assertion validation BFT access was granted and the service was called. Before sending BFT response to the Swedish client, PEP was responsible for preparing appropriate SAML assertion embedded in the SOAP response message. After receiving BFT response, STS analyzed SAML assertion prepared at the Polish side. Similar checking workflow was executed by STS module and in case of any incompatibilities BFT, access was not granted and the client was informed about that.

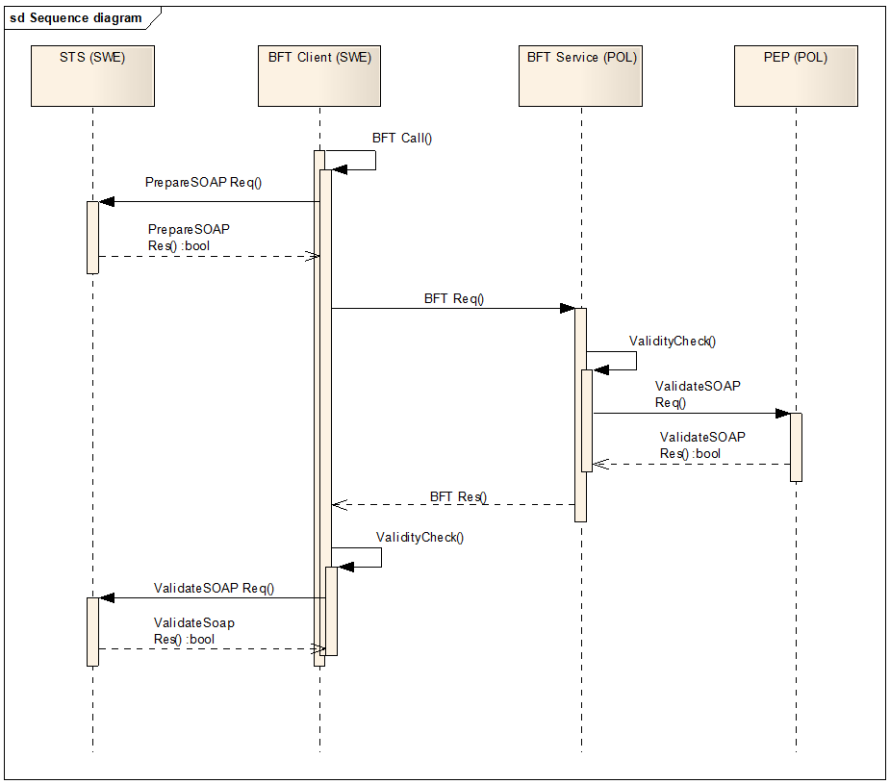

Fig. 9 Basic test scenario sequence diagram

The second scenario was very similar to the mentioned above. Security services were used in this case to provide cross-domain access control to the Query by Example services (QbE) implemented at both sides. This scenario tested bidirectional cooperation (SWE service – POL client, POL service – SWE client).

In third scenario QbE service was called indirect through semantic search service. Details regarding implementation and working of semantic search are out of scope of this article but positive results of tests prove proper work of security solutions.

It should be emphasized that all the tests were successful. During preparation phase for these experiments the teams agreed on the solution and set the SAML assertion specification for the purpose of the trial. Implementations of PEP and STS security modules were independent, without the necessity of sharing any piece of code.

5.0 WAY FORWARD / FURTHER WORKS

The solution presented in the article provides basic cross-domain authentication allowing to make authorization decisions locally, in the domain of the service provider. It relies on the trust between cooperating domains and supports the following security goals:

- Authentication in the domain of the user which can be verified in the domain of the service;
- Local authorization in the domain of the service;
- Integrity of the SOAP messages;
- Non-repudiation of sending the message.

The work under cross-domain security is a broad subject that should be deeply analysed in multinational communities and experimented frequently in order to find the most suitable solution, acceptable for every nation, easy for implementation and interoperable in heterogeneous environment. The work under these issues in MCI is being continued to provide coherent solution for cross-domain secure information exchange in SOA-based dynamic environment. Currently we are at the stage of making arrangements for tests of security solutions with the NC3A Core Services Testbed, which will be carried out in 2010.

The first step forward is to test cross-domain authentication of users which utilize different intradomain authentication methods, e.g. login/password, Kerberos and biometric data. These authentication methods should be appropriately identified by the authorization service and reflected in the local security policy.

When dealing with the web services security it needs to be emphasised that the publish-subscribe mode of operation should also be reflected. Since in this case the roles of the service and the client are reversed (client has the service interface listening for notifications, the service has the client side sending notifications) validity of the assertion and the user certificate should be also checked during the subscription period.

Another issue worth considering, and very much visible in the web service environment is the concept and implementation of service chaining and single-sign-on mechanisms. Service chaining is being used more and more often in service orchestration and is an intrinsic feature of the SOA-based world. In order to guarantee appropriate authentication, authorization, integrity and non-repudiation of sending the message there needs to be a mechanism providing identity delegation in the chain of services allowing to recognize the initiator of the process and grant access to the service based on his credentials.

In the area of reliability of information exchange there needs to be emphasised the need for combining the mechanism providing security and quality of service. In this area the work is conducted in scope of:

- Joint Security and QoS Policy for application and network layer resources access control and
- Dynamic Policy modification according to changing conditions e.g. : risk evaluation, detected threats and changing situation.
- Access control rules (Policy) negotiation between autonomous systems using XACML before they start information exchange.

BIBLIOGRAPHY

[1] Guide to Secure Web Services, NIST Special Publication 800-95, August 2007

[2] Securing NATO Web Services Across Domains – Federated Identity Management in an SOA Environment, James Bush, January 2008-08-20

[3] NATO Network Enabled Feasibility Study Volume I: Overview of the NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions, version 2.0

[4] NATO Network Enabled Feasibility Study Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII), version 2.0

[5] NEC Security Research Strategy, RTO-TR-IST-045 Technical Report

[6] J.J. Brennan Information Assurance for SOA, The Mitre Corporation, 2009

[7] ITU-T Recommendation X.805 - Security architecture for systems providing end-to-end communications

[8] Assertions and Protocols for the OASIS, Security Assertion Markup Language, (SAML) V2.0, OASIS Standard, 15 March 2005http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[9] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, 2008.